|  |  |
| --- | --- |
|  |  |
|  |  |

|  |
| --- |
| **Version 3** |
|  |

Privatinstitutionen Vandpytten

**Sikkerhedsprocedure**

**HANDLINGSPLAN**

**Datasikkerhedsbrud eller mistænkt datasikkerhedsbrud**

Et brud eller et muligt brud opdages af en ansat i institutionen eller en databehandler, alternativt at en af disse på anden vis bliver bekendt med et sådant brud.

**Hvad skal den ansatte/databehandler gøre?**

Ved mistanke om et brud på persondatasikkerheden sendes de fornødne informationer straks til institutionens responshold. Følgende informationer skal for så vidt muligt fremsendes:

1. Tidspunkt for opdagelsen af det potentielle brud
2. Omstændighederne ved bruddet
3. Hvilke personoplysninger bruddet omfatter
4. Hvor mange personers oplysninger er omfattet af bruddet
5. Mulige konsekvenser af bruddet
6. Øvrige informationer af relevans
7. Kontaktoplysninger

**Hvad skal responsholdet gøre?**

1. En person på responsholdet vurderer, om der er sket et brud på datasikkerheden.
2. I bekræftende fald, samles responsholdet og koordinerer håndteringen.
   * 1. Begræns bruddet
     2. Vurder bruddet
     3. Meddel bruddet
     4. Vurder og lær af bruddet

Indholdsfortegnelse

[1. Datasikkerhedsbrud/mistænkt datasikkerhedsbrud 4](#_Toc22633503)

[2. Hvad skal medarbejderen/databehandleren gøre? 6](#_Toc22633505)

[3. Hvad skal responsholdet gøre? 7](#_Toc22633506)

[1) Begræns bruddet 8](#_Toc22633507)

[2) Vurder bruddet 9](#_Toc22633508)

[3) Meddel bruddet 9](#_Toc22633509)

[**Anmeldelse til den national tilsynsmyndighed** 9](#_Toc22633510)

[*Skal der ske anmeldelse?* 10](#_Toc22633511)

[*Hvordan anmeldes bruddet til den nationale tilsynsmyndighed* 11](#_Toc22633512)

[*Tidspunktet for anmeldelse* 11](#_Toc22633513)

[*Anmeldelsens indhold* 11](#_Toc22633514)

[*Øvrige forhold som responsholdet har fokus på* 12](#_Toc22633515)

[**Underretning af den registrerede** 12](#_Toc22633516)

[*Skal der ske underretning?* 12](#_Toc22633517)

[*Tidspunktet for underretning* 13](#_Toc22633518)

[*Underretningens indhold* 13](#_Toc22633519)

[**Underretning til øvrige** 14](#_Toc22633520)

[**Løbende opsyn** 14](#_Toc22633521)

[4) Vurder og lær af bruddet 14](#_Toc22633522)

[4. Sikkerhedsbrudsfortegnelse 15](#_Toc22633523)

# 1. Datasikkerhedsbrud/mistænkt datasikkerhedsbrud

Institutionens ansatte skal være oplært og dermed i stand til at identificere et potentielt brud på persondatasikkerheden, herunder særligt forhindre et sådant ved den enkeltes egen behandling af personoplysninger, der behandles på vegne af institutionen.

Institutionen skal i den henseende indskærpe over for dets ansatte, at det er den enkelte ansats ansvar, at overholde nærværende sikkerhedsbrudsprocedure, idet en tilsidesættelse af institutionens forpligtelse kan medføre en bøde på op mod € 10 mio. eller 2 % af institutionens samlede globale årlige omsætning i det forudgående regnskabsår, såfremt dette beløb er højere[[1]](#footnote-1).

På den baggrund tjener nedenstående formålet, at sætte den ansatte i stand til at identificere et potentielt sikkerhedsbrud, da institutionen ikke kan håndtere et brud på persondatasikkerheden, hvis de ansatte ikke er i stand til at genkende et.

Et brud på persondatasikkerheden defineres i udgangspunktet af Databeskyttelsesforordningen, men ligeledes er en informationssikkerhedshændelse tillige et brud. Sidstnævnte defineres af ISO 27000-standarden[[2]](#footnote-2).

Definitionen, der fremgår af Databeskyttelsesforordningen, er følgende: ”*et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet*”[[3]](#footnote-3).

Institutionen har af hensyn til den ansattes overblik udfærdiget nedenstående figur, der udgør de forskellige muligheder for sikkerhedsbrud, dog ekskl. en informationssikkerhedshændelse.

Figuren benyttes ved at forbinde mindst en kasse fra hver kolonne hele vejen gennem figuren. Såfremt den ansatte er i stand til dette ud fra de faktiske omstændigheder, vil der være et potentielt brud på persondatasikkerheden, hvorefter den ansatte skal rette henvendelse til institutionens responshold.

Eksempel 1: Hvis en ansat ved en fejl (*hændelig, 1. kolonne*) fremsender en e-mail (*transmitteret, 4. kolonne*), der indeholder personoplysninger (*af personoplysninger, 3. kolonne*) til en forkert modtager (*uautoriseret videregivelse, 2. kolonne*) uden e-mailen er end-to-end krypteret, vil der potentielt være tale om et sikkerhedsbrud.

Eksempel 2: Hvis hackere (*ulovlig, 1. kolonne*)opnår adgang (*adgang, 2. kolonne*) til de personoplysninger (*til personoplysninger, 3. kolonne*), der er lagret på institutionens servere (*opbevaret, 4. kolonne*), vil der tillige potentielt være tale om et sikkerhedsbrud.

Institutionens sikkerhedsbrudsfigur er følgende:

Af/til personoplysninger der er

Opbevaret

På anden måde behandlet

Transmitteret

Tilintetgørelse

Ændring

Adgang

Uautoriseret videregivelse

Tab

Hændelig

Ulovlig

Den ansatte skal være særligt opmærksom på 3. kolonne, netop at det potentielle brud skal omhandle en eller flere personoplysninger[[4]](#footnote-4). Der er alene tale om en personoplysning, hvis samtlige af følgende kriterier er opfyldt: 1) Enhver form for information[[5]](#footnote-5), 2) om en[[6]](#footnote-6), 3) identificeret eller identificerbar[[7]](#footnote-7) 4) fysisk person[[8]](#footnote-8).

Datatilsynet har i dets vejledning[[9]](#footnote-9), anført at et brud på persondatasikkerheden f.eks. kan ske rent teknisk, hvis Institutionens IT-systemer med personoplysninger ikke er tilstrækkelig sikret, således udefrakommende får adgang til oplysningerne (f.eks. hacking). Det kan imidlertid også være institutionens egen håndtering af personoplysningerne, der kan forårsage et brud, f.eks. hvis institutionens ansatte ubeføjet videregiver eller ændrer personoplysningerne. Et andet eksempel, når det gælder institutionens egen håndtering af personoplysningerne er, hvis institutionen ulovligt eller som følge af et hændeligt uheld (f.eks. brand eller oversvømmelse) i en periode ikke har adgang til eller ender med at tilintetgøre personoplysningerne.

Såfremt den ansatte opnår kendskab til et potentielt brud på persondatasikkerheden, skal den pågældende følge institutionens retningslinje, der fremgår straks nedenfor.

# 2. Hvad skal medarbejderen/databehandleren gøre?

Den ansatte skal, hvis muligt, stoppe det potentielle brud på persondatasikkerheden straks, medmindre dette medfører, at institutionens dokumentation mistes eller får øvrige konsekvenser. Eksempelvis skal den ansatte kontakte brandvæsen først i tilfælde af brand, ligesom fysiske dokumenter skal forsøges reddet ved et sprængt vandrør.

Herefter skal den ansatte straks tage personlig eller telefonisk kontakt til et eller flere medlemmer af institutionens responshold. Responsholdet består af en række ansatte, der er oplistet i institutionens persondatapolitik. Henvendelsen sker med henblik på at varsle responsholdet om den indkomne anmeldelse.

Efterfølgende skal den ansatte udfylde nedenstående skema og fremsende den interne anmeldelse til det medlem fra responsholdet, som den ansatte har haft kontakt med. Den ansattes formalistiske benyttelse af institutionens skema er af underordnet betydning, da det vigtigste forbliver at den ansatte oplyser responsholdet om samtlige af de indholdspunkter, som skemaet indeholder.

Institutionens skema til brug for interne anmeldelser er følgende:

|  |  |
| --- | --- |
| Tidspunkt for opdagelsen af det potentielle brud | [Tidspunktet er vigtigt, da fristen for anmeldelse af bruddet til Datatilsynet starter fra dette tidspunkt. Det er derfor vigtigt at responsholdet kender til tidspunktet, således de kan overholde fristen.] |
| En beskrivelse af bruddets omstændigheder | [Den ansatte skal afgive samtlige informationer om den potentielle brud, således responsholdet opnår mest mulig viden herom, fx tyveriet er begået i weekenden, hvor der ikke har været nogle ansatte på kontoret. Gerningsmændene fik adgang via hoveddøren, som var sparket ind osv.] |
| Hvilke personoplysninger bruddet omfatter | [Den ansatte skal give så detaljerede informationer som muligt, såsom CPR-nr., oplysninger om strafbare forhold, da e-mail f.eks. indeholdt en ikke ”ren” straffeattest osv.] |
| Hvor mange personers oplysninger er omfattet af bruddet |  |
| Mulige konsekvenser af bruddet | [Hvis CPR-numre er stjålet vil det være en mulig konsekvens, at personoplysningen benyttes til identitetstyveri, ligeledes vil reg.nr. og konto nr. kunne bruges til økonomisk kriminalitet.] |
| Øvrige informationer af relevans | [Det kan fx være at der er opsat overvågningskameraer.] |
| Kontaktoplysninger | [Den ansatte arbejds- og private kontaktoplysninger, således responsholdet kan etablere kontakt til den ansatte, selv i weekenden, da responsholdet i udgangspunktet skal anmelde bruddet til Datatilsynet inden for 72 timer.] |
| Hvilke foranstaltninger er der truffet? | [Den ansatte skal oplyse om, hvilke sikkerhedsforanstaltninger, der er truffet, såsom at institutionens kontor var sikret ved ny lås efter indbrud eller serverne er slukket efter et opdaget hackerangreb.] |

# 3. Hvad skal responsholdet gøre?

Medlemmet fra institutionens responshold, der modtager anmeldelse fra institutionens egen ansat, dets databehandlere eller en tredjemand, skal foretage den foreløbige vurdering af, om der er sket et brud på persondatasikkerheden.

Vurderer det pågældende medlem, at der ikke er sket et brud, noteres dette, og der træffes ikke yderligere foranstaltninger. Medlemmet skal herefter indføje hændelsen i responsholdets fortegnelse for sikkerhedsbrud, der har til formål at dokumentere alle brud på persondatasikkerheden over for Datatilsynet, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger[[10]](#footnote-10). Dokumentationen skal mindst opbevares i 5 år, regnet fra tidspunktet for hvert enkelt sikkerhedsbrud[[11]](#footnote-11).

Det pågældende medlem skal efterfølgende orientere de øvrige medlemmer af institutionens responshold, således de orienteres om hændelsen samt opnår mulighed for at vurdere om de er enige i medlemmets kvalificering af hændelsen. I tilfældet, hvor medlemmerne er uenige om hændelsen udgør et brud på persondatasikkerheden eller ej, skal der indgives anmeldelse til Datatilsynet.

Såfremt det pågældende medlem konstaterer, at der er sket et brud på persondatasikkerheden, tager medlemmet kontakt til de øvrige medlemmer af responsholdet, hvorefter responsholdet foretager en indledende koordinering af rollefordelingen, og laver en kort handlingsplan, der iagttager institutionens pålagte tidsfrister[[12]](#footnote-12).

Institutionen bemærker, at brud på datasikkerheden kan have vekslende karakter, hvorfor det findes nødvendigt at lave en individuel handlingsplan på basis af hvert enkelt tilfælde. Grundet den hastende karakter vil disse ikke nødvendigvis forekomme skriftligt.

Handlingsplanen omfatter overordnet 4 trin[[13]](#footnote-13).

1. Begræns bruddet og foretag en indledende vurdering til dette formål
2. Vurder risikoen forbundet med bruddet
3. Meddel bruddet til de relevante
4. Vurder og lær af bruddet for at sikre imod fremtidige brud

Dokumenterne, som dannes af responsholdet samt andre oplysninger, der dokumenterer brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger gemmes. Dokumentationen skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at Databeskyttelsesforordningen er overholdt, og dokumenterne opbevares til dette formål[[14]](#footnote-14). Dokumentationen skal mindst opbevares i 5 år, regnet fra tidspunktet for hvert enkelt sikkerhedsbrud[[15]](#footnote-15).

## Begræns bruddet

Indledningsvist skal responsholdet søge at begrænse bruddet. Da brud på persondatasikkerheden kan forekomme i et utal af situationer, må der dannes en strategi for begrænsningen af hvert enkelt brud. For at danne en korrekt strategi vil følgende spørgsmål kunne anvendes af holdet.

* Hvordan opstod databruddet?
* Er personoplysningerne stadig i gang med at blive delt, offentliggjort eller slettet?
* Hvem har adgang til personoplysningerne?
* Hvad kan der gøres for at sikre personoplysningerne eller stoppe den uautoriserede adgang eller deling og reducere risikoen for skade på de påvirkede individer?

På baggrund af førnævnte må responsholdet vurdere, om holdet selv kan begrænse bruddet, eller om der skal tages kontakt til politi, bygningssikkerhed, personer hvis personoplysninger er blevet berørt af bruddet, modtagere af personoplysningerne i forbindelse med bruddet osv.

I forbindelse med begrænsningen af bruddet skal der udvises ekstrem varsomhed, såfremt noget ønskes slettet, da dette kan udgøre bevismateriale.

## Vurder bruddet

Responsholdets anden opgave er at vurdere bruddet. Vurderingen skal lede til en forståelse for risikoen, der er forbundet med bruddet.

Indledningsvist skal holdet indsamle informationer, således der kan skabes et situationsbillede af bruddet. Dette kan eventuelt gøres ved at referere til den modtagne anmeldelse fra institutionens egne ansatte eller dets databehandler. Herefter må de relevante personer kontaktes.

Informationerne skal for så vidt muligt omfatte:

* Dato, klokkeslæt, varighed og placering af bruddet
* Typen af personoplysninger omfattet af bruddet
* Hvordan og af hvem blev bruddet opdaget
* Grundlaget for og rækkevidden af bruddet
* En liste over de påvirkede personer, eller muligt påvirkede personer
* Risikoen for skade på de påvirkede personer
* Risikoen for andre skader

Førnævnte informationer skal samlet kunne give en udefrakommende, såsom Datatilsynet, et komplet billede af bruddet. På baggrund heraf må det igen vurderes, om der kan træffes foranstaltninger, der kan begrænse bruddet.

Endeligt sikres det at de fornødne dokumenter, som er forbundet med bruddet, samt responsholdets handlinger opbevares, da materialet skal benyttes som dokumentation over for Datatilsynet.

## Meddel bruddet

På tidspunktet, hvor responsholdet – eventuelt med bistand fra andre - har begrænset bruddet, og der er skabt et overblik over bruddet, skal holdet vurdere, om bruddet skal meddeles.

Der eksisterer flere meddelelsespligter, som forpligter institutionen til at give meddelelse til både de enkelte registrerede og myndigheder, såsom Datatilsynet. At give meddelelse om et brud kan være en vigtig hjælp til at sikre imod følgeskader af et brud på persondatasikkerheden. Modsat kan meddelelser om brud medføre unødigt utryghed. Unødige meddelelser vil også kunne gøre den registrerede mere ufølsom overfor eventuelle fremtidige meddelelsers vigtighed.

Responsholdet må derfor træffes en beslutning om meddelelse på baggrund af de konkrete omstændigheder forbundet med hvert enkelt brud på persondatasikkerheden.

### **Anmeldelse til den national tilsynsmyndighed**

Institutionens virksomhed ligger i Danmark, hvor Datatilsynet er den kompetente tilsynsmyndighed.

### *Skal der ske anmeldelse?*

Hvorvidt der skal ske anmeldelse af bruddet til Datatilsynet afhænger af, om bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder[[16]](#footnote-16).

Kommer responsholdets medlemmer enstemmigt frem til konklusionen, at risikoen er usandsynlig og derfor undlader at anmelde bruddet, er det institutionen som dataansvarlig, der bærer bevisbyrden for dette. Til hjælp for vurderingen kan responsholdet inddrage, om bruddet har medført en risiko for diskrimination, identitetstyveri eller –svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt og enhver anden væsentlig økonomisk eller social ulempe for den registrerede.

I denne vurdering bør der, når det er relevant, ses på følgende forhold:

1. Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse: I tilfældet, hvor der er udført et hackerangreb mod specifikke personoplysninger, vil risikoen være langt højere, end hvis en ansat har sendt en intern mail med personoplysninger til en forkert kollega, som ikke er autoriseret til at modtage personoplysningerne. Et brud, der indebærer, at personoplysninger ikke længere er tilgængelige, kan ligeledes få nogle helt andre konsekvenser for den registrerede, end hvis der f.eks. er tale om et brud, der resulterer i offentliggørelse af personoplysninger.
2. Personoplysningernes art og omfang: Personoplysninger, der er særligt beskyttelsesværdige, såsom fortrolige- og følsomme personoplysninger, CPR-numre samt oplysninger om strafbare forhold, vil medføre en større risiko end almindelige personoplysninger, såsom navn og adresse, eller personoplysninger, der i forvejen er offentlig tilgængelige.
3. Risikoen for at registrerede kan identificeres: Hvis institutionen har krypteret eller pseudonymiseret personoplysningerne, kan det medføre, at personoplysningerne ikke umiddelbart kan henføres til den registrerede, og derved formindske risikoen.
4. Alvorligheden af konsekvenserne for de berørte personer: Hvilke konsekvenser kan bruddet få for den enkelte registrerede? Her må ses på den enkelte registreredes omstændigheder og hvem de er, for at gøre det muligt at vurdere konsekvensernes betydning for denne.
5. Hvorvidt bruddet omfatter særlige registrerede: Det bør overvejes, hvorvidt de registrerede, som er omfattet af et brud er børn eller særligt udsatte personer. Det kunne have relevans f.eks. i en situation, hvor der sker offentliggørelse af adresse- eller kontaktoplysninger på en person, som er offentligt kendt og vil kunne møde større chikaner som resultat af bruddet.
6. Antallet af berørte fysiske personer: Antallet af berørte kan også have betydning, og det bør tages med i vurderingen.

### *Hvordan anmeldes bruddet til den nationale tilsynsmyndighed*

Skal bruddet anmeldes, skal dette ske på følgende link:

<https://www.datatilsynet.dk/anmeld-brud-paa-persondatasikkerheden/>

### *Tidspunktet for anmeldelse*

Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer[[17]](#footnote-17), efter at responsholdet er blevet bekendt med bruddet[[18]](#footnote-18).

Vurderingen af om anmeldelsen er sket *uden unødig forsinkelse* tager højde for karakteren og alvoren af bruddet og dets konsekvenser og skadevirkninger. Det er med andre ord en konkret vurdering, som tager højde for, at der skal være mulighed for at begrænse skadevirkningen.

Kan anmeldelse ikke nås indenfor 72 timer giver Databeskyttelsesforordningen to muligheder. Enten skal anmeldelsen, når den finder sted, ledsages af en begrundelse for forsinkelsen[[19]](#footnote-19). Alternativt kan der ske trinvis anmeldelse[[20]](#footnote-20). En trinvis anmeldelse skal tilstræbes.

### *Anmeldelsens indhold*

Anmeldelsen skal som minimum:

1. beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger,
2. angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes, altså responsholdets kontaktoplysninger,
3. beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden,

1. beskrive de foranstaltninger, som responsholdet på vegne af institutionen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

### *Øvrige forhold som responsholdet har fokus på*

Indebærer bruddet en risiko for registrerede i flere EU-medlemslande, skal dette oplyses til Datatilsynet i anmeldelsen.

### **Underretning af den registrerede**

### *Skal der ske underretning?*

Hvorvidt der skal ske en anmeldelse af bruddet til de registrerede afhænger af, om bruddet på persondatasikkerheden indebærer en høj risiko for fysiske personers rettigheder eller frihedsrettigheder[[21]](#footnote-21).

Vurderingen om bruddet indebærer en høj risiko er sammenfaldende med den vurdering, som responsholdet skal foretage i forbindelse med en anmeldelse til Datatilsynet, men underretningspligten har flere undtagelsesmuligheder.

Såfremt responsholdets medlemmer enstemmigt finder, at der ikke er en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske underretning af de enkelte registrerede, medmindre Datatilsynet pålægger institutionen at gøre dette.

Modsat, hvis et eller flere af responsholdets medlemmer finder, at der er en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, eksisterer der dog fortsat en række undtagelser i forhold til hovedreglen om underretningspligten. Undtagelserne er følgende:

Undtagelse 1 Hvis institutionen forinden bruddet har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, der f.eks. gør de berørte personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil (f.eks. ved kryptering), skal der ikke ske underretning[[22]](#footnote-22).

Eksemplificeret kunne en ansat glemme en usb-nøgle, hvorpå der var lagret personoplysninger, i et tog. Denne hændelse vil udgøre et sikkerhedsbrud. Hvis oplysningerne var meget beskyttelsesværdige, vil der kunne være en høj risiko for den registreredes rettigheder. Hvis personoplysningerne er krypterede tilstrækkeligt sikret, vil der ikke nødvendigvis være en høj risiko længere, hvorfor der ikke vil skulle foretages underretning.

Undtagelse 2 Responsholdet på vegne af institutionen eller dets databehandlere har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko sandsynligvis ikke længere er reel[[23]](#footnote-23).

Eksemplificeret, hvis en fejl offentliggør nogle personoplysninger på en hjemmeside, som ikke måtte offentliggøres. Responsholdet får fjernet de berørte personoplysninger meget kort tid herefter og gennemfører efterfølgende en undersøgelse, som definitivt viser at personoplysningerne ikke nåede at blive tilgået af besøgende på hjemmesiden.

Undtagelse 3 Såfremt underretningen ville kræve en uforholdsmæssig indsats af institutionen[[24]](#footnote-24).

Eksemplificeret, hvor der mistes rådigheden over samtlige forældreoplysninger i forbindelse med, at institutionens intranet rammes af ransomware. Når underretning vil kræve en uforholdsmæssig indsats, skal der i stedet gives en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

### *Tidspunktet for underretning*

Responsholdet skal give den enkelte registrerede underretning uden unødig forsinkelse. Hermed menes, at underretninger til registrerede bør gives, så snart det med rimelighed må anses for muligt. I vurderingen skal indgå den registreredes mulighed for at foretage beskyttende foranstaltninger, såsom mulighed for at ændre password m.v. hurtigt.

### *Underretningens indhold*

Responsholdets underretningen skal som minimum indeholde de følgende tre punkter, som er identiske med nogle af informationerne, der skal gives til Datatilsynet[[25]](#footnote-25). Underretningen skal indeholde følgende:

1. angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes, altså kontaktoplysningerne for institutionens responshold,
2. beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden,
3. beskrive de foranstaltninger, som responsholdet på vegne af institutionen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

### **Underretning til øvrige**

Det skal endeligt vurderes, om underretning skal ske til øvrige myndigheder, f.eks. politiet.

### **Løbende opsyn**

Såfremt det vurderes, at der ikke skal ske anmeldelse af et brud, vil der, såfremt det findes relevant, løbende blive ført opsyn med bruddet, da risikoen for fysiske personers rettigheder eller frihedsrettigheder kan ændre sig med tiden og dermed kræve en anmeldelse.

## Vurder og lær af bruddet

Til slut færdiganalyseres grundlaget for bruddet, og dette føres til en fortegnelse over brud på persondatastikkerheden, som holdes. Denne fortegnelse indeholder:

* Dato og tidspunkt for bruddet
* En beskrivelse af bruddet
* Årsagen til bruddet
* Typer af personoplysninger omfattet af bruddet
* Bruddets konsekvenser for de berørte personer
* Hvilke afhjælpende foranstaltninger der er truffet
* Hvorvidt der er sket anmeldelse til Datatilsynet eller ej
* Begrundelser for responsholdets væsentlige beslutninger som følge af bruddet. Dette kan f.eks. være, hvorfor det er besluttet, at der ikke skal ske anmeldelse af et brud på persondatasikkerheden til Datatilsynet.

På baggrund af erfaringerne vil der om nødvendigt ske en opdatering af sikkerhed og sikkerhedsbrudsproceduren. Der vil også kunne ske ændringer af politikker og procedurer i institutionen. Herudover kan yderligere oplæring af personale blive aktuelt.

Responsholdet fremsætter, når det er relevant, forslag for instutionens øverste ledelse.

# 4. Sikkerhedsbrudsfortegnelse

|  |  |
| --- | --- |
| **Fortegnelse for sikkerhedsbrud**  - for hvilke instutionen er dataansvarlig for | |
| I. Dato og tidspunkt for bruddet: |  |
| II. De faktiske omstændigheder ved bruddet (hvad er der sket?) |  |
| III. Årsagen til bruddet? |  |
| IV. Hvilken type personoplysninger er berørt? |  |
| V. Hvilke konsekvenser har bruddet for de berørte personer? |  |
| VI. Hvilke afhjælpende foranstaltninger er truffet? |  |
| **VII. Underretning?** | |
| VIII.I Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår?) |  |
| VIII.II Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet? |  |
| IX.I Er der sket underretning af de berørte personer (hvis ja, hvornår?) |  |
| IX.II Hvis nej, begrundelse for ikke at underrette de berørte personer? |  |

1. Databeskyttelsesforordningens artikel 83, stk. 4. [↑](#footnote-ref-1)
2. ”En identificeret forekomst af en system-, tjeneste- eller netværkstilstand, der indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af kontroller, eller en tidligere ukendt situation der kan være relevant for sikkerheden …” [↑](#footnote-ref-2)
3. Databeskyttelsesforordningens artikel 4, nr. 12. [↑](#footnote-ref-3)
4. En personoplysning er i Databeskyttelsesforordningens artikel 4, nr. 1 defineret som ”*enhver form for information om en identificeret eller identificerbar fysisk person*.” [↑](#footnote-ref-4)
5. Der er tale om en bred definition, idet alle informationer er omfattet. [↑](#footnote-ref-5)
6. Informationen skal være henførbare, således information kan henføres til den pågældende person. [↑](#footnote-ref-6)
7. Informationen skal angå en identificeret (direkte) eller identificerbar person (indirekte). Hvornår er en person identificerbar? Ifølge Databeskyttelsesforordningens præambel nr. 26 fremgår det, at ved afgørelsen om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person. Dermed skal der ikke meget til, før en person kan identificeres. F.eks. hvis navnet erstattes af en kode eller initialer, vil der stadig være tale om en personoplysning, såfremt koden kan føres tilbage til den oprindelige individuelle personoplysning.

   Et eksempel der kan illustrere dette er arbejdsmails. Anders Andersen kan have en arbejdsmail, som hedder AA@arbejde.dk. Alene mailadressen viser ikke, at det er Anders Andersens mail. Men på arbejdets hjemmeside kan man finde Anders Andersens profil, som indeholder navn og mail. Dermed kan der med en let søgen identificeres, at mailadressen AA@arbejde.dk er Anders Andersens arbejdsmail. [↑](#footnote-ref-7)
8. Alene informationer om fysiske personer er omfattet. Såfremt den pågældende er en juridisk person, såsom aktieselskaber, anpartsselskaber, kommanditselskaber, fonde, foreninger og visse selvejende institutioner m.v., vil der ikke være tale om en fysisk person. Øvrige juridiske personer, såsom enkeltmandsvirksomhed og interessentskaber udgør fysiske personer. Levende personer er omfattet, uanset om de er frataget den retlige handleevne, hvorfor der er tale om en fysisk person. Afdøde personers informationer er omfattet af loven 10 år efter vedkommendes død. Fostre er ikke afklaret, men det antages, at de vil være en fysisk person. [↑](#footnote-ref-8)
9. Vejledning om håndtering af brud på persondatasikkerheden, s. 4. [↑](#footnote-ref-9)
10. Databeskyttelsesforordningens artikel 33, stk. 5. [↑](#footnote-ref-10)
11. Databeskyttelseslovens § 41, stk. 7. [↑](#footnote-ref-11)
12. Databeskyttelsesforordningens artikel 33, stk. 1. [↑](#footnote-ref-12)
13. Nogle af disse trin vil afhængigt af bruddets karakter ske overlappende eller i kort forlængelse af hinanden. Trinnene kan også tænkes at være overflødige i undtagelsestilfælde, og i andre tilfælde kan der være behov for at inddrage yderligere trin. [↑](#footnote-ref-13)
14. Databeskyttelsesforordningens artikel 33, stk. 5. [↑](#footnote-ref-14)
15. Databeskyttelseslovens § 41, stk. 7. [↑](#footnote-ref-15)
16. Databeskyttelsesforordningens artikel 33, stk. 1. [↑](#footnote-ref-16)
17. Databeskyttelsesforordningens artikel 33, stk. 1. [↑](#footnote-ref-17)
18. Fristen løber ikke fra der opstår en formodning om et brud, men først fra tidspunktet, hvor institutionen blev bekendt med bruddet. [↑](#footnote-ref-18)
19. Databeskyttelsesforordningens artikel 33, stk. 1, 2. pkt. [↑](#footnote-ref-19)
20. Databeskyttelsesforordningens artikel 33, stk. 4. [↑](#footnote-ref-20)
21. Databeskyttelsesforordningens artikel 34, stk. 1. [↑](#footnote-ref-21)
22. Databeskyttelsesforordningens artikel 34, stk. 3, litra a. [↑](#footnote-ref-22)
23. Databeskyttelsesforordningens artikel 34, stk. 3, litra b. [↑](#footnote-ref-23)
24. Databeskyttelsesforordningens artikel 34, stk. 3, litra c. [↑](#footnote-ref-24)
25. Databeskyttelsesforordningens artikel 34, stk. 2. [↑](#footnote-ref-25)